

COMPUTING NÉRON–SEVERI GROUPS AND CYCLE CLASS GROUPS

BJORN POONEN, DAMIANO TESTA, AND RONALD VAN LUIJK

ABSTRACT. Assuming the Tate conjecture and the computability of étale cohomology with finite coefficients, we give an algorithm that computes the Néron–Severi group of any smooth projective geometrically integral variety, and also the rank of the group of numerical equivalence classes of codimension p cycles for any p .

1. INTRODUCTION

Let k be a field, and let k^{sep} be a separable closure. Let X be a smooth projective geometrically integral k -variety, and let $X^{\text{sep}} := X \times_k k^{\text{sep}}$.

If $k = \mathbb{C}$, then the Lefschetz $(1, 1)$ theorem identifies the Néron–Severi group $\text{NS } X$ (see Section 3 for definitions) with the subgroup of $H^2(X(\mathbb{C}), \mathbb{Z})$ mapping into the subspace $H^{1,1}(X)$ of $H^2(X(\mathbb{C}), \mathbb{C})$. Analogously, if k is a finitely generated field, then the Tate conjecture describes $(\text{NS } X^{\text{sep}}) \otimes \mathbb{Q}_\ell$ in terms of the action of $\text{Gal}(k^{\text{sep}}/k)$ on $H_{\text{ét}}^2(X^{\text{sep}}, \mathbb{Q}_\ell(1))$, for any prime $\ell \neq \text{char } k$.

Can such descriptions be transformed into algorithms for computing $\text{NS } X^{\text{sep}}$? To make sense of this question, we assume that k is replaced by a finitely generated subfield over which X is defined; then X and k admit a finite description suitable for computer input (see Section 7.1). Using the Lefschetz $(1, 1)$ theorem involves working over the uncountable field \mathbb{C} , while using the Tate conjecture involves an action of an uncountable Galois group on a vector space over an uncountable field \mathbb{Q}_ℓ , so it is not clear a priori that either approach can be made into an algorithm.

In this paper, assuming only the ability to compute the finite Galois modules $H_{\text{ét}}^2(X^{\text{sep}}, \mu_{\ell^n})$ for each n , we give an algorithm for computing $\text{NS } X^{\text{sep}}$ that terminates if and only if the Tate conjecture holds for X (Remark 8.23). Moreover, if k is finite, then we can even avoid computing the Galois modules $H_{\text{ét}}^2(X^{\text{sep}}, \mu_{\ell^n})$, by instead using point-counting to compute the zeta function of X , as is well known (Theorem 8.25(b)). Combining this with the truth of the Tate conjecture for K3 surfaces X over finite fields of characteristic at least 5 ([Nyg83, NO85, Mau12, Cha12]) yields an unconditional algorithm for computing $\text{rk NS } X^{\text{sep}}$ for such X (Corollary 8.27). (See [Tat94, Section 5] and [And96] for some other cases in which the Tate conjecture is known.) We also provide an unconditional algorithm for computing the torsion subgroup $(\text{NS } X^{\text{sep}})_{\text{tors}}$ for any X over any finitely generated field k (Theorem 8.21).

Date: December 15, 2012.

2010 *Mathematics Subject Classification.* Primary 14C22; Secondary 14C25, 14F20, 14G13.

Key words and phrases. Néron–Severi groups, cycle class groups, Tate conjecture.

B.P. was supported by the Guggenheim Foundation and National Science Foundation grants DMS-0841321 and DMS-1069236.

Finally, we prove also statements for cycles of higher codimension. In particular, we describe a conditional algorithm that computes the rank of the group $\text{Num}^p X^{\text{sep}}$ of codimension p cycles modulo numerical equivalence (Theorem 8.5).

If k^{sep} is replaced by an algebraic closure \bar{k} in any of the results above, the resulting analogue holds (Remarks 8.6 and 8.24).

2. PREVIOUS APPROACHES

Several techniques exist in the literature for obtaining information on Néron–Severi groups:

- Lower bounds on the rank are often obtained by exhibiting divisors explicitly.
- An initial upper bound is given by the second Betti number, which is computable.
- Over \mathbb{C} , Hodge theory provides the improved upper bound h^{11} , which again is computable.
- Over a finite field k , computation of the zeta function can yield an improved upper bound: see Section 8.4 for details.
- Over finitely generated fields k , one can spread out X to a smooth projective scheme \mathcal{X} over a finitely generated \mathbb{Z} -algebra and reduce modulo maximal ideals to obtain injective specialization homomorphisms $(\text{NS } X^{\text{sep}}) \otimes \mathbb{Q} \rightarrow (\text{NS } \mathcal{X}_{\bar{F}}) \otimes \mathbb{Q}$ where F is the finite residue field (see [vL07b, Proposition 6.2] or [MP12, Proposition 3.6], for example). Combining this with the method of the previous item bounds the rank of $\text{NS } X^{\text{sep}}$. In some cases, one can prove directly that certain elements of $(\text{NS } \mathcal{X}_{\bar{F}}) \otimes \mathbb{Q}$ are not in the image of the specialization homomorphism, to improve the bound [EJ11b].
- The previous item can be improved also by using more than one reduction if one takes into account that the specialization homomorphisms preserve additional structure, such as the intersection pairing in the case $\dim X = 2$ [vL07] or the Galois action [EJ11]. In the $\dim X = 2$ case, the discriminant of the intersection pairing can be obtained, up to a square factor, either from explicit generators for $(\text{NS } \mathcal{X}_{\bar{F}}) \otimes \mathbb{Q}$ [vL07] or from the Artin–Tate conjecture [Klo07]. F. Charles proved that for a K3 surface X over a number field, the information from reductions is sufficient to determine the rank of $\text{NS } X^{\text{sep}}$, assuming the Hodge conjecture for 2-cycles on $X \times X$ [Cha11].
- If X is a quotient of another variety Y by a finite group G , then the natural map $(\text{NS } X^{\text{sep}}) \otimes \mathbb{Q} \rightarrow ((\text{NS } Y^{\text{sep}}) \otimes \mathbb{Q})^G$ is an isomorphism. For instance, this has been applied to **Delsarte surfaces**, i.e., surfaces in \mathbb{P}^3 defined by a homogeneous form with four monomials, using that they are quotients of Fermat surfaces [Shi86].
- When X is an elliptic surface, the rank of $\text{NS } X^{\text{sep}}$ is related to the rank of the Mordell–Weil group of the generic fiber [Tat95, p. 429; Shi72, Corollary 1.5; Shi90, Corollary 5.3]. This has been generalized in various ways, for example to fibrations into abelian varieties [Kah09; Ogu09, Theorem 1.1].
- When X is a K3 surface of degree 2 over a number field, the Kuga–Satake construction relates the Hodge classes on X to the Hodge classes on an abelian variety of dimension 2^{19} . B. Hassett, A. Kresch, and Yu. Tschinkel use this to give an algorithm to compute $\text{NS } X^{\text{sep}}$ for such X [HKT12, Proposition 19].

3. NOTATION

Given a module A over an integral domain R , let A_{tors} be its torsion submodule, let $\tilde{A} := A/A_{\text{tors}}$, and let $\text{rk } A := \dim_K(A \otimes_R K)$ where $K := \text{Frac } R$. If A is a submodule of another R -module B , the **saturation** of A in B is $\{b \in B : nb \in A \text{ for some nonzero } n \in R\}$. If A is a G -module for some group G , then A^G is the subgroup of invariant elements. We say that a G -module A is **finite** (resp. **finitely generated**) if it is so as a set (resp. abelian group).

Given a field k , let \bar{k} be an algebraic closure, let k^{sep} be the separable closure inside \bar{k} , let $G_k := \text{Gal}(k^{\text{sep}}/k) \simeq \text{Aut}(\bar{k}/k)$, and let κ be the characteristic of k . A **variety** X over a field k is a separated scheme of finite type over k . For such X , let $X^{\text{sep}} := X \times_k k^{\text{sep}}$ and $\bar{X} := X \times_k \bar{k}$. Call X **nice** if it is smooth, projective, and geometrically integral.

Suppose that X is a nice k -variety. Let $\text{Pic } X$ be its **Picard group**. Let $\mathbf{Pic}_{X/k}$ be the **Picard scheme** of X over k . There is an injection $\text{Pic } X \rightarrow \mathbf{Pic}_{X/k}(k)$, but it is not always surjective. Let $\mathbf{Pic}_{X/k}^0$ be the connected component of the identity in $\mathbf{Pic}_{X/k}$. Let $\text{Pic}^0 X \leq \text{Pic } X$ be the group of isomorphism classes of line bundles such that the corresponding k -point of $\mathbf{Pic}_{X/k}$ lies in $\mathbf{Pic}_{X/k}^0$; any such line bundle \mathcal{L} (or divisor representing it) is called **algebraically equivalent to 0**. Equivalently, a line bundle \mathcal{L} is algebraically equivalent to 0 if there is a connected variety B and a line bundle \mathcal{M} on $X \times B$ such that \mathcal{M} restricts to the trivial line bundle above one point of B and to \mathcal{L} above another (this holds even over the ground field k : take B to be a component H of \mathbf{EffDiv}_X lying above a translate of $\mathbf{Pic}_{X/k}^0$ as in Lemma 8.18(a,b)). Define the **Néron–Severi group** $\text{NS } X$ as the quotient $\text{Pic } X / \text{Pic}^0 X$; it can be identified with the set of components of $\mathbf{Pic}_{X/k}$ containing the class of a divisor of X over k (which is stronger than assuming that the component has a k -point). Then $\text{NS } X$ is a finitely generated abelian group [Nér52, p. 145, Théorème 2] (see [SGA 6, XIII.5.1] for another proof). Let $\mathbf{Pic}_{X/k}^\tau$ be the finite union of connected components of $\mathbf{Pic}_{X/k}$ parametrizing classes of line bundles whose class in $\text{NS } \bar{X}$ is torsion.

Let $\mathcal{Z}^p(X)$ be the group of codimension p cycles on X . Let $\text{Num}^p X$ be the quotient of $\mathcal{Z}^p(X)$ by the subgroup of cycles numerically equivalent to 0. Then $\text{Num}^p X$ is a finite-rank free abelian group. Let $\mathcal{Z}^1(X)^\tau$ be the set of divisors $z \in \mathcal{Z}^1(X)$ having a positive multiple that is algebraically equivalent to 0. Let $(\text{Pic } X)^\tau$ be the image of $\mathcal{Z}^1(X)^\tau$ under $\mathcal{Z}^1(X) \rightarrow \text{Pic } X$.

If $m \in \mathbb{Z}_{>0}$ and $\kappa \nmid m$, and $i, p \in \mathbb{Z}$, let $H^i(X^{\text{sep}}, (\mathbb{Z}/m\mathbb{Z})(p))$ be the étale cohomology group; this is a finite abelian group. For each prime $\ell \neq \kappa$, define $H^i(X^{\text{sep}}, \mathbb{Z}_\ell(p)) := \varprojlim_n H^i(X^{\text{sep}}, (\mathbb{Z}/\ell^n\mathbb{Z})(p))$, a finitely generated \mathbb{Z}_ℓ -module; and define $H^i(X^{\text{sep}}, \mathbb{Q}_\ell(p)) := H^i(X^{\text{sep}}, \mathbb{Z}_\ell(p)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, a finite-dimensional \mathbb{Q}_ℓ -vector space.

4. GROUP-THEORETIC LEMMAS

Given any prime ℓ , let $\ell' := \ell$ if $\ell \neq 2$, and $\ell' := 4$ if $\ell = 2$.

Lemma 4.1 (cf. [Min87, §1]). *Let ℓ be a prime. Let G be a group acting through a finite quotient on a finite-rank free \mathbb{Z} -module or \mathbb{Z}_ℓ -module Λ . If G acts trivially on $\Lambda/\ell'\Lambda$, then G acts trivially on Λ .*

Proof. Let $n := \text{rk } \Lambda$. Write $\ell' =: \ell^s$. For $r \geq s$, let $U_r := 1 + \ell^r M_n(\mathbb{Z}_\ell)$. It suffices to show that there are no non-identity elements of finite order in the kernel U_s of $\text{GL}_n(\mathbb{Z}_\ell) \rightarrow \text{GL}_n(\mathbb{Z}_\ell/\ell'\mathbb{Z}_\ell)$. In fact, for $r \geq s$ the binomial theorem shows that $1 + A \in U_r - U_{r+1}$ implies

$(1 + A)^\ell \in U_{r+1} - U_{r+2}$, so by induction any non-identity $1 + A \in U_s$ has infinitely many distinct powers, and cannot be of finite order. \square

Lemma 4.2. *Let a topological group G act continuously on a finite-rank free \mathbb{Z}_ℓ -module Λ . Let $r := \text{rk } \Lambda^G$. Then the following hold.*

- (a) *The continuous cohomology group $H^1(G, \Lambda)[\ell^\infty]$ is finite.*
- (b) *$\#(\Lambda/\ell^n \Lambda)^G = O(\ell^{rn})$ as $n \rightarrow \infty$.*

Proof. For each n , taking continuous group cohomology of $0 \rightarrow \Lambda \xrightarrow{\ell^n} \Lambda \rightarrow \Lambda/\ell^n \Lambda \rightarrow 0$ yields

$$0 \rightarrow \frac{\Lambda^G}{\ell^n(\Lambda^G)} \rightarrow \left(\frac{\Lambda}{\ell^n \Lambda} \right)^G \rightarrow H^1(G, \Lambda)[\ell^n] \rightarrow 0. \quad (4.3)$$

- (a) By (4.3) for $n = 1$, the group $H^1(G, \Lambda)[\ell]$ is finite. So if $H^1(G, \Lambda)[\ell^\infty]$ is infinite, it contains a copy of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, contradicting the $Y = 0$ case of [Tat76, Proposition 2.1].
- (b) In (4.3), the group on the left has size ℓ^{rn} , and the group on the right has size $O(1)$ as $n \rightarrow \infty$, by (a). \square

5. UPPER BOUND ON THE RANK OF THE GROUP OF TATE CLASSES

Setup 5.1. Let k be a finitely generated field. Let $G := G_k$. Let X be a nice variety over k . Let $d := \dim X$. Fix $p \in \{0, 1, \dots, d\}$. For each $m \in \mathbb{Z}_{>0}$ with $\kappa \nmid m$, define $T_m := H^{2p}(X^{\text{sep}}, (\mathbb{Z}/m\mathbb{Z})(p))$. Fix a prime $\ell \neq \kappa$. Define $T := H^{2p}(X^{\text{sep}}, \mathbb{Z}_\ell(p))$, and $V := H^{2p}(X^{\text{sep}}, \mathbb{Q}_\ell(p))$.

An element of V is called a **Tate class** if it is fixed by a (finite-index) open subgroup of G . Let $V^{\text{Tate}} \leq V$ be the \mathbb{Q}_ℓ -subspace of Tate classes. Let M be the \mathbb{Z}_ℓ -submodule of elements of T mapping to Tate classes in V . Let $r := \text{rk } M = \dim V^{\text{Tate}}$.

Lemma 5.2. *For each $n \geq 0$, there is an exact sequence*

$$0 \rightarrow \frac{T}{\ell^n T} \rightarrow T_{\ell^n} \rightarrow H^{2p+1}(X^{\text{sep}}, \mathbb{Z}_\ell(p))[\ell^n] \rightarrow 0.$$

Proof. Use [Mil80, Lemma V.1.11] to take cohomology of

$$0 \rightarrow \mathbb{Z}_\ell(p) \xrightarrow{\ell^n} \mathbb{Z}_\ell(p) \rightarrow (\mathbb{Z}/\ell^n \mathbb{Z})(p) \rightarrow 0. \quad \square$$

Corollary 5.3. *For each $n \geq 0$, there is a canonical injection $M/\ell^n M \hookrightarrow T_{\ell^n}$.*

Proof. Since M is saturated in T , we have an injection $M/\ell^n M \hookrightarrow T/\ell^n T$. Compose with the first map in Lemma 5.2. \square

Lemma 5.4. *Assume that G acts trivially on $T_{\ell'}$.*

- (a) *For any $n \geq 0$, we have $\#T_{\ell^n}^G \geq \ell^{rn}$.*
- (b) *We have $\#T_{\ell^n}^G = O(\ell^{rn})$ as $n \rightarrow \infty$.*

Proof. By Corollary 5.3, G acts trivially on $M/\ell' M$, and hence also on $M/\ell M$ and $\widetilde{M}/\ell' \widetilde{M}$.

- (a) Also by Corollary 5.3, $\#T_{\ell^n}^G \geq \#(M/\ell^n M)^G$. We now prove $\#(M/\ell^n M)^G \geq \ell^{rn}$ by induction on n . For $n = 0$, this is $1 \geq 1$. For $n > 0$, the group $\ell^{n-1} M/\ell^n M$ is a

homomorphic image of $M/\ell M$, so G acts trivially on $\ell^{n-1}M/\ell^n M$, which has size at least ℓ^r . Now taking G -invariants of

$$0 \rightarrow \frac{\ell^{n-1}M}{\ell^n M} \rightarrow \frac{M}{\ell^n M} \rightarrow \frac{M}{\ell^{n-1}M} \rightarrow 0$$

yields the inductive step.

- (b) The G -orbit of each element of \widetilde{M} is finite by definition of Tate class, and \widetilde{M} is finitely generated as a \mathbb{Z}_ℓ -module, so G acts through a finite quotient on \widetilde{M} . By Lemma 4.1, G acts trivially on \widetilde{M} . By definition of M , we have $\widetilde{T}^G \subseteq \widetilde{M} = \widetilde{M}^G \subseteq \widetilde{T}^G$, so $\text{rk } \widetilde{T}^G = r$. Dividing the first two terms in Lemma 5.2 by the images of T_{tors} yields

$$0 \rightarrow \frac{\widetilde{T}}{\ell^n \widetilde{T}} \rightarrow \frac{T_{\ell^n}}{I_n} \rightarrow H^{2p+1}(X^{\text{sep}}, \mathbb{Z}_\ell(p))[\ell^n] \rightarrow 0,$$

where I_n is the image of T_{tors} in T_{ℓ^n} . This implies the second inequality in

$$\#T_{\ell^n}^G \leq \#I_n^G \cdot \# \left(\frac{T_{\ell^n}}{I_n} \right)^G \leq \#I_n^G \cdot \# \left(\frac{\widetilde{T}}{\ell^n \widetilde{T}} \right)^G \cdot \# (H^{2p+1}(X^{\text{sep}}, \mathbb{Z}_\ell(p))[\ell^n])^G.$$

Since $H^i(X^{\text{sep}}, \mathbb{Z}_\ell(p))$ is a finitely generated \mathbb{Z}_ℓ -module for each i , the first and third factors on the right are $O(1)$. On the other hand, Lemma 4.2(b) yields $\#(\widetilde{T}/\ell^n \widetilde{T})^G = O(\ell^{rn})$. Multiplying shows that $\#T_{\ell^n}^G = O(\ell^{rn})$. \square

Proposition 5.5. *Assume that G acts trivially on T_ℓ . Then*

$$r = \min \left\{ \left\lfloor \frac{\log \#T_{\ell^n}^G}{\log \ell^n} \right\rfloor : n \geq 1 \right\}.$$

Proof. This is a corollary of Lemma 5.4. \square

6. CYCLES UNDER FIELD EXTENSION

In this section, assume Setup 5.1.

Proposition 6.1.

- (a) *For any extension L of k , the natural map $\text{Num}^p X \rightarrow \text{Num}^p X_L$ is injective.*
- (b) *The image of $\text{Num}^p X \rightarrow \text{Num}^p \overline{X}$ is a finite-index subgroup of $(\text{Num}^p \overline{X})^G$.*
- (c) *If $\kappa > 0$, the index of $\text{Num}^p X^{\text{sep}}$ in $\text{Num}^p \overline{X}$ is finite and equal to a power of κ .*

The same three statements hold for NS instead of Num^p .

Proof.

- (a) If $z \in \mathcal{Z}^p(X)$ has intersection number 0 with all p -cycles on X_L , then in particular it has intersection number 0 with all p -cycles on X .
- (b) Suppose that $[z] \in (\text{Num}^p \overline{X})^G$, where $z \in \mathcal{Z}^p(\overline{X})$. Then z comes from some $z_L \in \mathcal{Z}^p(X_L)$ for some finite extension L of k . Let $n := [L : k]$. Then $n[z] = \text{tr}_{L/k}[z]$ comes from $\text{tr}_{L/k} z_L \in \mathcal{Z}^p(X)$. Hence the cokernel of $\text{Num}^p X \rightarrow (\text{Num}^p \overline{X})^G$ is torsion, but it is also finitely generated, so it is finite.
- (c) We may assume that $k = k^{\text{sep}}$. Then $G = \{1\}$, so (b) implies that $\text{Num}^p X^{\text{sep}}$ is of finite index in $\text{Num}^p \overline{X}$. Moreover, in the proof of (b), $[L : k]$ is always a power of κ , so the index is a power of κ .

Statement (a) for NS follows from the fact that the formation of $\mathbf{Pic}_{X/k}^0$ respects field extension [Kle05, Proposition 9.5.3]. The proofs of (b) and (c) for NS are the same as for Num^p . \square

Proposition 6.2. *If k is finite, then the natural homomorphisms $\text{Pic } X \rightarrow (\text{Pic } X^{\text{sep}})^G$ and $\text{NS } X \rightarrow (\text{NS } X^{\text{sep}})^G$ are isomorphisms.*

Proof. That $\text{Pic } X \rightarrow (\text{Pic } X^{\text{sep}})^G$ is an isomorphism follows from the Hochschild–Serre spectral sequence for étale cohomology and the vanishing of the Brauer group of k . Lang’s theorem [Lan56] implies $H^1(k, \text{Pic}^0 X^{\text{sep}}) = 0$, so taking Galois cohomology of

$$0 \rightarrow \text{Pic}^0 X^{\text{sep}} \rightarrow \text{Pic } X^{\text{sep}} \rightarrow \text{NS } X^{\text{sep}} \rightarrow 0$$

shows that the homomorphism $\text{Pic } X = (\text{Pic } X^{\text{sep}})^G \rightarrow (\text{NS } X^{\text{sep}})^G$ is surjective. On the other hand, its image is $\text{NS } X$. \square

7. HYPOTHESES AND CONJECTURES

Our computability results rely on the ability to compute étale cohomology with finite coefficients. Some of the results are conditional also on the Tate conjecture and related conjectures. We now formulate these hypotheses precisely, so that they can be referred to in our main theorems.

7.1. Explicit representation of objects. To specify an ideal in a polynomial ring over \mathbb{Z} in finitely many indeterminates, we give a finite list of generators. To specify a finitely generated \mathbb{Z} -algebra A , we give an ideal I in a polynomial ring R as above such that A is isomorphic to R/I . To specify a finitely generated field k , we give a finitely generated \mathbb{Z} -algebra A that is a domain such that k is isomorphic to $\text{Frac } A$. To specify a continuous G_k -action on a finitely generated abelian group A , we give a finite Galois extension k' of k together with an action of $\text{Gal}(k'/k)$ on A such that there exists a k -embedding $k' \hookrightarrow k^{\text{sep}}$ such that the original G_k -action is the composition $G_k \twoheadrightarrow \text{Gal}(k'/k) \rightarrow \text{Aut } A$. To specify a G_k -action on finitely many finitely generated abelian groups, we use the same k' for all of them. To specify a projective variety X , we give its homogeneous ideal for a particular embedding of X in some projective space. To specify a codimension p cycle on X , we give an explicit integer combination of codimension p integral subvarieties of X .

Definition 7.1. Given k , X , and p as in Setup 5.1, to compute a G_k -module homomorphism f from $\mathcal{Z}^p(X^{\text{sep}})$ to an (abstract) finitely generated G_k -module A means to compute

- a finite Galois extension k' of k ,
- an explicit finitely generated $\text{Gal}(k'/k)$ -module A' , and
- an algorithm that takes as input a finite separable extension L of k' and an element of $\mathcal{Z}^p(X_L)$ and returns an element of A' ,

such that there exists a k -embedding $k' \hookrightarrow k^{\text{sep}}$ and an isomorphism $A' \xrightarrow{\sim} A$ such that the composition $\mathcal{Z}^p(X_L) \rightarrow A' \xrightarrow{\sim} A$ factors as $\mathcal{Z}^p(X_L) \rightarrow \mathcal{Z}^p(X^{\text{sep}}) \xrightarrow{f} A$ for some (or equivalently, every) k' -embedding $L \hookrightarrow k^{\text{sep}}$.

Remark 7.2. A similar definition can be made for G_k -module homomorphisms defined only on a G_k -submodule of $\mathcal{Z}^p(X^{\text{sep}})$.

7.2. Hypotheses.

Hypothesis 7.3 (Cohomology is computable). *Given (k, X, p, ℓ) as in Setup 5.1 and $n \in \mathbb{Z}_{\geq 0}$, we can compute a finite G_k -module isomorphic to $H^{2p}(X^{\text{sep}}, (\mathbb{Z}/\ell^n \mathbb{Z})(p))$.*

It seems reasonable to expect that Hypothesis 7.3 is in reach of existing methods, although it has not been verified yet.

See [Tat94] for a survey of the relationships between the following two conjectures and many others.

Conjecture $T^p(X, \ell)$ (Tate conjecture). *Assume Setup 5.1. The cycle class homomorphism*

$$\mathcal{Z}^p(X^{\text{sep}}) \otimes \mathbb{Q}_\ell \rightarrow V^{\text{Tate}}$$

is surjective.

Conjecture $E^p(X, \ell)$ (Numerical equivalence equals homological equivalence). *Assume Setup 5.1. An element of $\mathcal{Z}^p(X^{\text{sep}})$ is numerically equivalent to 0 if and only if its class in V is 0.*

Remark 7.4. Conjecture $E^1(X, \ell)$ holds (see [Tat94, p. 78]).

Given (k, p, X, ℓ) as in Setup 5.1, with k finite, let V_μ be the largest G -invariant subspace of V on which all eigenvalues of the Frobenius are roots of unity. We have $V^{\text{Tate}} \leq V_\mu$.

Proposition 7.5. *Fix X , p , and ℓ , and assume Conjecture $E^p(X, \ell)$. Then the following integers are equal:*

- (a) *the \mathbb{Z} -rank of the G_k -module $\text{Num}^p X^{\text{sep}}$,*
- (b) *the \mathbb{Z} -rank of the image of $\mathcal{Z}^p(X^{\text{sep}})$ in V , and*
- (c) *the \mathbb{Q}_ℓ -dimension of the image of $\mathcal{Z}^p(X^{\text{sep}}) \otimes \mathbb{Q}_\ell$ in V .*

The integer in (c) is less than or equal to the following equal integers,

- (d) *the \mathbb{Q}_ℓ -dimension of V^{Tate} and*
- (e) *the \mathbb{Z}_ℓ -rank of the G_k -module M of Section 5,*

which, if k is finite, are less than or equal to

- (f) *the \mathbb{Q}_ℓ -dimension of V_μ .*

If moreover, $T^p(X, \ell)$ holds, then all the integers (including (f) if k is finite) are equal. Conversely, if (c) equals (d), then $T^p(X, \ell)$ holds.

Proof. The only nontrivial statements are

- the equality of (b) and (c), which is [Tat94, Lemma 2.5], and
- the fact that $T^p(X, \ell)$ and $E^p(X, \ell)$ for k finite together imply the equality of (d) and (f); this follows from [Tat94, Theorem 2.9, (b) \Rightarrow (c)].

□

8. ALGORITHMS

8.1. Computing $\text{Num}^p X^{\text{sep}}$. Throughout this section, we assume Setup 5.1.

Lemma 8.1. *There is an algorithm that takes as input k , p , X , and cycles $z \in \mathcal{Z}^p(X)$ and $y \in \mathcal{Z}^{d-p}(X)$, and returns the intersection number $z.y$.*

Proof. First, if z and y are integral cycles intersecting properly, use Gröbner bases to compute the degree of their scheme-theoretic intersection. If z and y are arbitrary cycles whose supports intersect properly, use bilinearity to reduce to the previous sentence. In general, search for a rational equivalence between z and another p -cycle z' such that the supports of z' and y intersect properly; eventually z' will be found; then apply the previous sentence to compute $z'.y$. \square

The following lemma describes a decision problem for which we do not have an algorithm that always terminates, but only a *one-sided* test, i.e., an algorithm that halts if the answer is YES, but runs forever without reaching a conclusion if the answer is NO.

Lemma 8.2. *There is an algorithm that takes as input k, p, X , a finite extension L of k , and a finite list of cycles $z_1, \dots, z_s \in \mathcal{Z}^p(X_L)$, and halts if and only if the images of z_1, \dots, z_s in $\text{Num}^p \overline{X}$ are \mathbb{Z} -independent.*

Proof. Enumerate s -tuples (y_1, \dots, y_s) of elements of $\mathcal{Z}^{d-p}(X_{L'})$ as L' ranges over finite separable extensions of L . As each s -tuple is computed, compute also the intersection numbers $y_i.z_j \in \mathbb{Z}$ and halt if $\det(y_i.z_j) \neq 0$. \square

Remark 8.3. In Lemma 8.2, if L is separable over k , then it would be the same to ask for independence in $\text{Num}^p X^{\text{sep}}$, by Proposition 6.1(a).

Corollary 8.4. *There is an algorithm that takes as input k, p , and X , and that when left running forever, prints out an infinite sequence of nonnegative integers whose maximum equals $\text{rk Num}^p X^{\text{sep}}$.*

Proof. Enumerate finite s -tuples (z_1, \dots, z_s) of elements of $\mathcal{Z}^p(X_L)$ for all $s \geq 0$ and all finite separable extensions L of k , and run the algorithm of Lemma 8.2 (using Remark 8.3) on all of them in parallel, devoting a fraction 2^{-i} of the algorithm's time to the i^{th} process. Each time one of the processes halts, print its value of s . \square

Theorem 8.5 (Computing $\text{Num}^p X^{\text{sep}}$).

- (a) *Assume Hypothesis 7.3. Then there is an algorithm that takes as input (k, p, X, ℓ) as in Setup 5.1 such that, assuming $E^p(X, \ell)$,*
 - *the algorithm terminates if and only if $T^p(X, \ell)$ holds, and*
 - *if the algorithm terminates, it returns $\text{rk Num}^p X^{\text{sep}}$.*
- (b) *There is an unconditional algorithm that takes k, p, X , and a nonnegative integer ρ as input, and computes the following assuming that $\rho = \text{rk Num}^p X^{\text{sep}}$:*
 - (i) *a finitely generated torsion-free G_k -module N having a G_k -equivariant injection $\text{Num}^p X^{\text{sep}} \hookrightarrow N$ with finite cokernel,*
 - (ii) *the composition $\mathcal{Z}^p(X^{\text{sep}}) \rightarrow \text{Num}^p X^{\text{sep}} \hookrightarrow N$ in the sense of Definition 7.1, and*
 - (iii) *the rank of $\text{Num}^p X$.*

Proof.

- (a) Let ℓ' be as in Section 4. Use Hypothesis 7.3 to compute $T_{\ell'}$. Replace k by a finite Galois extension to assume that G_k acts trivially on $T_{\ell'}$. Let M and r be as in Section 5.

By day, use Hypothesis 7.3 to compute the groups T_{ℓ^n} , and the upper bounds $\lfloor \log \#T_{\ell^n}^G / \log \ell^n \rfloor$ on r given by Proposition 5.5. By night, compute lower bounds on $\text{rk Num}^p X^{\text{sep}}$ as in Corollary 8.4. Stop if the bounds ever match, which happens if and only if equality

holds in the inequality $\text{rk Num}^p X^{\text{sep}} \leq r$, which by Proposition 7.5 happens if and only if $T^p(X, \ell)$ holds. In this case, we have computed $\text{rk Num}^p X^{\text{sep}}$.

- (b) (i) Search for a finite Galois extension k' of k , for p -cycles y_1, \dots, y_s , and for codimension p cycles z_1, \dots, z_t over k' until the intersection matrix $(y_i \cdot z_j)$ has rank ρ . The assumption $\rho = \text{rk Num}^p X^{\text{sep}}$ guarantees that such k' , y_i , z_j will be found eventually. Let Y be the free abelian group with basis equal to the set consisting of the y_i and their Galois conjugates, so Y is a G_k -module. The intersection pairing defines a homomorphism $\phi: \text{Num}^p X^{\text{sep}} \rightarrow \text{Hom}_{\mathbb{Z}}(Y, \mathbb{Z})$ whose image has rank equal to $\rho = \text{rk Num}^p X^{\text{sep}}$. Since $\text{Num}^p X^{\text{sep}}$ is torsion-free, ϕ is injective. Compute the saturation N of the \mathbb{Z} -span of $\phi(z_1), \dots, \phi(z_s)$ in $\text{Hom}_{\mathbb{Z}}(Y, \mathbb{Z})$. Because of its rank, N equals the saturation of $\phi(\text{Num}^p X^{\text{sep}})$. Thus N is a finitely generated torsion-free G_k -module containing a finite-index G_k -submodule $\phi(\text{Num}^p X^{\text{sep}})$ isomorphic to $\text{Num}^p X^{\text{sep}}$.
- (ii) Given $z \in \mathcal{Z}^p(X_L)$ for some finite separable extension L of k' , computing its intersection number with each basis element of Y yields the image of z in N .
- (iii) Because of Proposition 6.1(b), $\text{rk Num}^p X = \text{rk } N^{G_k}$, which is computable. \square

Remark 8.6. The analogue of Theorem 8.5 with X^{sep} replaced by \overline{X} also holds. (By Proposition 6.1(c), $\text{Num}^p X^{\text{sep}}$ is of finite index in $\text{Num}^p \overline{X}$, so in the proof of Theorem 8.5(b)(i), the homomorphism ϕ extends to a G_K -equivariant injective homomorphism $\overline{\phi}: \text{Num}^p \overline{X} \rightarrow \text{Hom}_{\mathbb{Z}}(Y, \mathbb{Z})$. Because of finite index, the image of $\overline{\phi}$ is contained in N . The cokernel of $\text{Num}^p \overline{X} \rightarrow N$ is finite.

Remark 8.7. For each $p \in \{0, 1, \dots, d\}$, let N_p be the N in Theorem 8.5(b)(i), and define $Q_p := N_p \otimes \mathbb{Q}$. Then for any $p, q \in \mathbb{Z}_{\geq 0}$ with $p + q \leq d$, we can compute a bilinear pairing $Q_p \times Q_q \rightarrow Q_{p+q}$ that corresponds to the intersection pairing: indeed, each Q_p is spanned by classes of cycles, whose intersections in the Chow ring can be computed by an argument similar to that used to prove Lemma 8.1.

8.2. Checking algebraic equivalence of divisors.

Lemma 8.8. *There is an algorithm that takes as input k , X , a finite extension L of k , and an element $z \in \mathcal{Z}^1(X_L)$, and halts if and only if z is algebraically equivalent to 0.*

Proof. Enumerate all possible descriptions of an algebraic family of divisors on X_L with a pair of L -points of the base (it is easy to check when such a description is valid), and check for each whether the difference of the cycles corresponding to the two points equals z . \square

Lemma 8.9. *There is an algorithm that takes as input k , X , a finite extension L of k and $z \in \mathcal{Z}^1(X_L)$, and decides whether z lies in $\mathcal{Z}^1(X_L)^{\tau}$, i.e., whether the Néron–Severi class of z is torsion, i.e., whether z is numerically equivalent to 0.*

Proof. By day, search for a positive integer n and a family of divisors showing that nz is algebraically equivalent to 0. By night, run the algorithm of Lemma 8.2 for $s = 1$, which halts if and only if the image of z in $\text{Num}^1 \overline{X}$ is nonzero, i.e., if and only if $z \notin \mathcal{Z}^1(X_L)^{\tau}$. One of these processes will halt. \square

8.3. Computing the Néron–Severi group.

In this section, k is an arbitrary field.

Lemma 8.10.

- (a) Let X be a nice k -variety. There exists a divisor $B \in \mathcal{Z}_{X/k}^1$ such that for any ample divisor D , the class of $D + B$ is very ample.
- (b) There is an algorithm that takes as input a finitely generated field k and a k -variety X and computes a B as in (a).

Proof. Let K be a canonical divisor on X (this is computable if k is finitely generated). Let A be a very ample divisor on X (e.g., embed X in some projective space, and choose a hyperplane section). By [Kee08, Theorem 1.1(2)], $B := K + (\dim X + 1)A$ has the required property. \square

Given an effective Cartier divisor of X , we have an associated closed subscheme $Y \subseteq X$. Call a closed subscheme $Y \subseteq X$ a divisor if it arises this way. When we speak of the Hilbert polynomial of an effective Cartier divisor on a closed subscheme X of \mathbb{P}^n , we mean the Hilbert polynomial of the associated closed subscheme of X .

Lemma 8.11. *There is an algorithm that takes as input a finitely generated field k , a closed subscheme $X \subseteq \mathbb{P}_k^n$, and an effective divisor $D \subset X$, and computes the Hilbert polynomial of D .*

Proof. This is evident already from [Her26, Satz 2], which can be applied repeatedly to construct a minimal free resolution of \mathcal{O}_D . \square

Let $\text{Hilb } X = \bigcup_P \text{Hilb}_P X$ denote the Hilbert scheme of X , where P ranges over polynomials in $\mathbb{Q}[t]$.

Lemma 8.12. *There is an algorithm that takes as input a finitely generated field k , a closed subscheme $X \subseteq \mathbb{P}_k^n$, and a polynomial $P \in \mathbb{Q}[t]$, and computes the universal family $\mathcal{Y} \rightarrow \text{Hilb}_P X$.*

Proof. This is a consequence of work of Gotzmann. Let $S = \bigoplus_{d \geq 0} S_d := k[x_0, \dots, x_n]$, so $\text{Proj } S = \mathbb{P}_k^n$. Given $d, r \in \mathbb{Z}_{\geq 0}$, let $\text{Gr}_r(S_d)$ be the Grassmannian parametrizing r -dimensional subspaces of the k -vector space S_d . Then [Got78, §3] (see also [IK99, Theorem C.29 and Corollary C.30]) specifies $d_0 \in \mathbb{Z}_{\geq 0}$ such that for $d \geq d_0$, one can compute $r \in \mathbb{Z}_{\geq 0}$ and a closed subscheme $W \subseteq \text{Gr}_r(S_d)$ such that $W \simeq \text{Hilb}_P \mathbb{P}^n$; under this isomorphism a subspace $V \subseteq S_d$ corresponds to the subscheme defined by the ideal I_V generated by the polynomials in V . Moreover, I_V and its saturation have the same d^{th} graded part (see [IK99, Corollary C.18]).

Let f_1, \dots, f_m be generators of a homogeneous ideal defining X . Choose $d \in \mathbb{Z}$ such that $d \geq d_0$ and $d \geq \deg f_i$ for all i . Let g_1, \dots, g_M be all the polynomials obtained by multiplying each f_i by all monomials of degree $d - \deg f_i$. By the saturation statement above, $\text{Proj}(S/I_V) \subseteq X$ if and only if $g_j \in V$ for all j . This lets us construct $\text{Hilb}_P X$ as an explicit closed subscheme of $\text{Hilb}_P \mathbb{P}^n$. Now $\text{Hilb}_P X$ is known as an explicit subscheme of the Grassmannian, so we have explicit equations also for the universal family over it. \square

Lemma 8.13. *Let X be a nice k -variety. There exists an open and closed subscheme $\mathbf{EffDiv}_X \subseteq \text{Hilb } X$ such that for any field extension $L \supseteq k$ and any $s \in (\text{Hilb } X)(L)$, the closed subscheme of X_L corresponding to s is a divisor on X_L if and only if $s \in \mathbf{EffDiv}_X(L)$.*

Proof. See [BLR90, p. 215] for the definition of the functor \mathbf{EffDiv}_X (denoted there by $\text{Div}_{X/S}$ for $S = \text{Spec } k$) and its representability by an open subscheme of $\text{Hilb } X$. To see that

it is also closed, we apply the valuative criterion for properness to the inclusion $\mathbf{EffDiv}_X \rightarrow \mathbf{Hilb} X$: if a k -scheme S is the spectrum of a discrete valuation ring and Z is a closed subscheme of $X \times S$ that is flat over S and the generic fiber Z_η of $Z \rightarrow S$ is a divisor, then Z equals the closure of Z_η in $X \times S$, which is an effective Weil divisor on $X \times S$ and hence a relative effective Cartier divisor since $X \times S$ is regular. \square

The existence of the scheme \mathbf{EffDiv}_X in Lemma 8.13 immediately implies the following.

Corollary 8.14. *Let X be a nice k -variety. Let Y be a closed subscheme of X . Let L be a field extension of k . Then Y is a divisor on X if and only if Y_L is a divisor on X_L .*

Remark 8.15. Corollary 8.14 holds more generally for any finite-type k -scheme X , as follows from fpqc descent applied to the ideal sheaf of $Y_L \subseteq X_L$.

Lemma 8.16. *There is an algorithm that takes as input a finitely generated field k , a smooth k -variety X , and a closed subscheme $Y \subseteq X$, and decides whether Y is a divisor in X .*

Proof. By [EGA IV₄, Proposition 21.7.2] or [Eis95, Theorem 11.8a.], Y is a divisor if and only if all associated primes of Y are of codimension 1 in X . So choose an affine cover (X_i) of X , compute the associated primes of the ideal of $Y \cap X_i$ in X_i for each i (the first algorithm was given in [Her26]), and check whether they all have codimension 1 in X_i (a modern method for computing dimension uses that the Hilbert polynomial of an ideal equals the Hilbert polynomial of an associated initial ideal, which can be computed from a Gröbner basis). \square

Lemma 8.17. *Let $\pi: H \rightarrow P$ be a proper morphism of schemes of finite type over a field k . Suppose that the fibers of π are connected (in particular, nonempty). Then π induces a bijection on connected components.*

Proof. Let H_1, \dots, H_n be the connected components of H . Let $P_i := \pi(H_i)$, so P_i is connected. Since π is proper, the P_i are closed. Since the fibers of π are connected, the P_i are disjoint. Since the fibers are nonempty, $\bigcup P_i = P$. Since the P_i are finite in number, they are open too, so they are the connected components of P . \square

Let $\pi: \mathbf{EffDiv}_X \rightarrow \mathbf{Pic}_{X/k}$ be the proper morphism sending a divisor to its class. If $\mathbf{Pic}_{X/k}^c$ is a finite union of connected components of $\mathbf{Pic}_{X/k}$ and L is a field extension of k , let $\mathbf{Pic}^c X_L$ be the set of classes in $\mathbf{Pic} X_L$ such that the corresponding point of $(\mathbf{Pic}_{X/k})_L$ lies in $(\mathbf{Pic}_{X/k}^c)_L$, and let $\mathbf{NS}^c X_L$ be the image of $\mathbf{Pic}^c X_L$ in $\mathbf{NS} X_L$.

Lemma 8.18.

(a) *Let X be a nice k -variety. Let $\mathbf{Pic}_{X/k}^c$ be any finite union of connected components of $\mathbf{Pic}_{X/k}$. Assume the following:*

For every field extension $L \supseteq k$, every divisor on X_L with class in $\mathbf{Pic}^c X_L$ is linearly equivalent to an effective divisor. (8.19)

Let $H := \pi^{-1}(\mathbf{Pic}_{X/k}^c)$. Then $\pi: H(L) \rightarrow \mathbf{Pic} X_L$ induces a bijection

$\{\text{connected components of } H_L \text{ that contain an } L\text{-point}\} \longrightarrow \mathbf{NS}^c X_L$. (8.20)

(b) *For any $\mathbf{Pic}_{X/k}^c$ as in (a), there is a divisor F on X such that the translate $F + \mathbf{Pic}_{X/k}^c$ satisfies (8.19).*

- (c) *There is an algorithm that takes as input a finitely generated field k , a nice k -variety X , a divisor $D \in \mathcal{Z}^1(X)$, and a positive integer e , and computes the following for $\mathbf{Pic}_{X/k}^c$ defined as the (possibly empty) union of components of $\mathbf{Pic}_{X/k}$ corresponding to classes of divisors E over \bar{k} such that eE is numerically equivalent to D :*
- (i) *a divisor F as in (b) for $\mathbf{Pic}_{X/k}^c$,*
 - (ii) *the variety H in (a) for $F + \mathbf{Pic}_{X/k}^c$,*
 - (iii) *the universal family $Y \rightarrow H$ of divisors corresponding to points of H ,*
 - (iv) *a finite separable extension k' of k and a finite subset $\mathcal{S} \subseteq \mathcal{Z}^1(X_{k'})$ such that there exists a k -homomorphism $k' \hookrightarrow k^{\text{sep}}$ such that the composition $\mathcal{Z}^1(X_{k'}) \rightarrow \mathcal{Z}^1(X^{\text{sep}}) \rightarrow \text{NS } X^{\text{sep}}$ restricts to a bijection $\mathcal{S} \rightarrow \text{NS}^c X^{\text{sep}}$.*

Proof.

- (a) Taking $L = \bar{k}$ in (8.19) shows that $H \xrightarrow{\pi} \mathbf{Pic}_{X/k}^c$ is surjective. The fibers of $\pi: H(L) \rightarrow \text{Pic}^c X_L$ are linear systems, and are nonempty by (8.19), so the reduced geometric fibers of $\pi: H \rightarrow \mathbf{Pic}_{X/k}^c$ are projective spaces. In particular, $\pi_L: H_L \rightarrow (\mathbf{Pic}_{X/k}^c)_L$ has connected fibers, so by Lemma 8.17, it induces a bijection on connected components. Under this bijection, the connected components of H_L that contain an L -point map to the connected components of $(\mathbf{Pic}_{X/k}^c)_L$ containing the class of a divisor over L . The set of the latter components is $\text{NS}^c X_L$.
- (b) Let A be an ample divisor on X . For each of the finitely many geometric components C of $\mathbf{Pic}_{X/k}^c$, choose a divisor D_C on $X_{\bar{k}}$ whose class lies in C , and let $n_C \in \mathbb{Z}$ be such that $n_C A + D_C$ is ample. Let $n = \max n_C$, so $nA + D_C$ is ample for all C . Let B be as in Lemma 8.10(a). Let $F = B + nA$. If L is a field extension of k and E is a divisor on X_L with class in $\text{Pic}^c X_L$, let C be the geometric component containing the class of $E_{\bar{L}}$ (for some compatible choice of $\bar{k} \subseteq \bar{L}$); then E is numerically equivalent to D , so $nA + E$ is ample too, so $F + E = B + (nA + E)$ is very ample by choice of B , so $F + E$ is linearly equivalent to an effective divisor.
- (c) Fix a projective embedding of X , and let A be a hyperplane section.
 - (i) Let $n \in \mathbb{Z}_{>0}$ be such that $nA + D$ is ample. (To compute such an n , try $n = 1, 2, \dots$ until $|nA + D|$ determines a closed immersion.) Compute B as in Lemma 8.10(b). Let $F = B + nA$. Suppose that L is an extension of k and E is a divisor on X_L such that eE is numerically equivalent to D . Then $e(nA + E)$ is numerically equivalent to $enA + D = (e-1)nA + (nA + D)$, which is a positive combination of the ample divisors A and $nA + D$, so $nA + E$ is ample. By choice of B , the divisor $F + E = B + (nA + E)$ is very ample and hence linearly equivalent to an effective divisor.
 - (ii) By the Riemann–Roch theorem, the Euler characteristic $\chi(F + sD + tA)$ is a polynomial $f(s, t)$ of total degree at most $d := \dim X$. For any $s \in \mathbb{Z}$, we can compute $t \in \mathbb{Z}$ such that $F + sD + tA$ is linearly equivalent to an effective divisor, whose Hilbert polynomial can be computed by Lemma 8.11, so the polynomial $\chi(F + sD + tA)$ can be found by interpolation. Let $P(t) := f(1/e, t)$. Compute the universal family $\mathcal{Y} \rightarrow \text{Hilb}_P X$ as in Lemma 8.12. Suppose that E is such that eE is numerically equivalent to D . Then the polynomial $\chi(F + sE + tA)$ equals $f(s/e, t)$ since its values match whenever $e|s$. In particular, $\chi(F + E + tA) = P(t)$; i.e., $P(t)$ is the Hilbert polynomial of an effective

divisor linearly equivalent to $F + E$. Thus the subscheme $H \subseteq \mathbf{EffDiv}_X \subseteq \mathrm{Hilb} X$ is contained in $\mathrm{Hilb}_P X$, which is a union of connected components of $\mathrm{Hilb} X$. By definition, H is a union of connected components of \mathbf{EffDiv}_X , which by Lemma 8.13 is a union of connected components of $\mathrm{Hilb} X$, so H is a union of connected components of $\mathrm{Hilb}_P X$. To compute H , compute the (finitely many) connected components of $\mathrm{Hilb}_P X$; to check whether a component C belongs to H , choose a point h in C over some extension of k , apply Lemma 8.16 to \mathcal{Y}_h to test whether \mathcal{Y}_h is a divisor, and if so, apply Lemma 8.9 to $e\mathcal{Y}_h - D$ to check whether $e\mathcal{Y}_h$ is numerically equivalent to D .

- (iii) Compute $Y \rightarrow H$ as the part of $\mathcal{Y} \rightarrow \mathrm{Hilb}_P X$ above H .
- (iv) Compute the connected components of $H_{k^{\mathrm{sep}}}$, which really means computing a finite separable extension k' and the connected components of $H_{k'}$ such that these components are geometrically connected. For each connected component C of $H_{k'}$, use the algorithm of [Har88] to decide whether it has a k^{sep} -point, and, if so, choose a k' -point h of C , enlarging k' if necessary, and take the fiber Y_h . Let \mathcal{S} be the set of such divisors Y_h , one for each component C with a k^{sep} -point. By (a), the map $\mathcal{S} \rightarrow \mathrm{NS} X^{\mathrm{sep}}$ is a bijection onto $\mathrm{NS}^c X^{\mathrm{sep}}$. \square

Theorem 8.21 (Computing $(\mathrm{NS} X^{\mathrm{sep}})_{\mathrm{tors}}$). *There is an algorithm that takes as input a finitely generated field k and a nice k -variety X , and computes the G_k -homomorphism $\mathcal{Z}^1(X^{\mathrm{sep}})^{\tau} \rightarrow (\mathrm{NS} X^{\mathrm{sep}})_{\mathrm{tors}}$ sending a divisor to its Néron–Severi class, in the sense of Definition 7.1 and Remark 7.2.*

Proof. Apply Lemma 8.18(c) with $D = 0$ and $e = 1$ to obtain a finite Galois extension k' and a subset $\mathcal{D} \subseteq \mathcal{Z}^1(X_{k'})$ mapping bijectively to $(\mathrm{NS} X^{\mathrm{sep}})_{\mathrm{tors}}$. For each pair $D_1, D_2 \in \mathcal{D}$, run Lemma 8.8 in parallel on $D_1 + D_2 - D_3$ for all $D_3 \in \mathcal{D}$ to find the unique D_3 algebraically equivalent to $D_1 + D_2$; this determines the group law on \mathcal{D} . Similarly compute the G_k -action. Similarly, given a finite separable extension L of k' and $z \in \mathcal{Z}^1(X_L)^{\tau}$, we can find the unique $D \in \mathcal{D}$ algebraically equivalent to z . \square

If $\mathcal{D} \subseteq \mathcal{Z}^1(X_{k^{\mathrm{sep}}})$, let $(\mathrm{NS} X^{\mathrm{sep}})^{\mathcal{D}}$ be the saturation of the G_k -submodule generated by the image of \mathcal{D} in $\mathrm{NS} X^{\mathrm{sep}}$, and let $\mathcal{Z}^1(X^{\mathrm{sep}})^{\mathcal{D}}$ be the set of divisors in $\mathcal{Z}^1(X^{\mathrm{sep}})$ whose algebraic equivalence class lies in $(\mathrm{NS} X^{\mathrm{sep}})^{\mathcal{D}}$.

Theorem 8.22 (Computing $\mathrm{NS} X^{\mathrm{sep}}$).

- (a) *Given a finitely generated field k , a nice k -variety X , a finite separable extension L of k in k^{sep} and a finite subset $\mathcal{D} \subseteq \mathcal{Z}^1(X_L)$, we can compute the G_k -homomorphism $\mathcal{Z}^1(X^{\mathrm{sep}})^{\mathcal{D}} \rightarrow (\mathrm{NS} X^{\mathrm{sep}})^{\mathcal{D}}$ in the sense of Definition 7.1 and Remark 7.2.*
- (b) *There is an algorithm that takes as input k and X as above and a nonnegative integer ρ , and computes the G_k -homomorphism $\mathcal{Z}^1(X^{\mathrm{sep}}) \rightarrow (\mathrm{NS} X^{\mathrm{sep}})$ in the sense of Definition 7.1 and Remark 7.2 assuming that $\rho = \mathrm{rk} \mathrm{NS} X^{\mathrm{sep}}$.*

Remark 8.23. Assume Hypothesis 7.3 and $T^1(X, \ell)$. (Conjecture $E^1(X, \ell)$ is proved.) Then Theorem 8.5(a) lets us compute $\mathrm{rk} \mathrm{NS} X^{\mathrm{sep}}$, so Theorem 8.22(b) lets us compute $\mathrm{NS} X^{\mathrm{sep}}$.

Proof of Theorem 8.22.

- (a) Enlarge L to assume that it is Galois over k , and replace \mathcal{D} by the union of its $\mathrm{Gal}(L/k)$ -conjugates. There exist $D_1, \dots, D_t \in \mathcal{D}$ whose images in $(\mathrm{Num}^1 X^{\mathrm{sep}}) \otimes \mathbb{Q}$ form a \mathbb{Q} -basis

for the image of the span of \mathcal{D} . Then there exist 1-dimensional cycles E_1, \dots, E_t on X_L such that $\det(D_i.E_j) \neq 0$ (the E_i exist over a finite extension of L , but can be replaced by their traces down to L), and each $D \in \mathcal{D}$ has a positive integer multiple numerically equivalent to an element of the \mathbb{Z} -span of \mathcal{D} . Search for such $D_1, \dots, D_t, E_1, \dots, E_t$ and for numerical relations as above for each $D \in \mathcal{D}$ (use Lemma 8.9 to verify relations). Let $e := |\det(D_i.E_j)|$. Let Δ be the span of the image of \mathcal{D} in $\text{Num}^1 X^{\text{sep}}$. Let Δ' be the saturation of Δ in $\text{Num}^1 X^{\text{sep}}$. Then $(\Delta' : \Delta)$ divides e . For each coset of $e\Delta$ in Δ , choose a representative divisor D in the \mathbb{Z} -span of \mathcal{D} , and check whether the set \mathcal{S} of Lemma 8.18(c) is nonempty to decide whether the numerical equivalence class of D is in $e\Delta'$; if so, choose a divisor in \mathcal{S} . The classes of these new divisors, together with those of D_1, \dots, D_t , generate Δ' . Moreover, we know the integer relations between all of these, so we can compute integer combinations F_1, \dots, F_t whose classes form a *basis* for Δ' . Then

$$(\text{NS } X^{\text{sep}})^{\mathcal{D}} \simeq (\mathbb{Z}F_1 \oplus \dots \oplus \mathbb{Z}F_t) \oplus (\text{NS } X^{\text{sep}})_{\text{tors}}$$

as abelian groups, and $(\text{NS } X^{\text{sep}})_{\text{tors}}$ can be computed by Theorem 8.21.

The homomorphism $\mathcal{Z}^1(X^{\text{sep}})^{\mathcal{D}} \rightarrow (\text{NS } X^{\text{sep}})^{\mathcal{D}}$ is computed as follows: given any $z \in \mathcal{Z}^1(X^{\text{sep}})^{\mathcal{D}}$ (defined over some finite separable extension L' of L in k^{sep}), compute an integer combination F of the F_i such that $F.E_j = z.E_j$ for all j , and apply the homomorphism of Theorem 8.21 to compute the class of $z - F$ in $(\text{NS } X^{\text{sep}})_{\text{tors}}$.

Applying this to all conjugates of our generators of $(\text{NS } X^{\text{sep}})^{\mathcal{D}}$ lets us compute the G_k -action on our model of $(\text{NS } X^{\text{sep}})^{\mathcal{D}}$.

- (b) Assuming that $\rho = \text{rk NS } X^{\text{sep}}$, the algebraic equivalence classes of divisors $D_1, \dots, D_\rho \in \mathcal{Z}^1(X^{\text{sep}})$ form a \mathbb{Z} -basis for a free subgroup of finite index in $\text{NS } X^{\text{sep}}$ if and only if there exist 1-cycles E_1, \dots, E_ρ on X^{sep} such that $\det(D_i.E_j) \neq 0$. Search for a finite separable extension L of k in k^{sep} , divisors $D_1, \dots, D_\rho \in \mathcal{Z}^1(X_L)$, and 1-cycles E_1, \dots, E_ρ on X_L until such are found with $\det(D_i.E_j) \neq 0$. Then apply (a) to $\mathcal{D} := \{D_1, \dots, D_\rho\}$. \square

Remark 8.24. Theorems 8.21 and 8.22 hold for \overline{X} instead of X^{sep} : the same proofs work, except that we need an algorithm for deciding whether a variety has a \overline{k} -point; fortunately, this is even easier than deciding whether a variety has a k^{sep} -point!

8.4. An alternative approach over finite fields. When k is a finite field, we can compute $\text{rk Num}^p X^{\text{sep}}$ without assuming Hypothesis 7.3, but still assuming $\text{T}^p(X, \ell)$ and $\text{E}^p(X, \ell)$. The arguments in this section are mostly well-known.

The following is a variant of Theorem 8.5(a).

Theorem 8.25.

- (a) *There is an algorithm A that takes as input (k, p, X, ℓ) as in Setup 5.1, with k a finite field \mathbb{F}_q , and returns $\dim V_\mu$.*
- (b) *There is an algorithm B that takes as input (k, p, X, ℓ) as in Setup 5.1, with k a finite field \mathbb{F}_q , such that, assuming $\text{E}^p(X, \ell)$,*
- algorithm B terminates on this input if and only if $\text{T}^p(X, \ell)$ holds, and*
 - if algorithm B terminates, it returns $\text{rk Num}^p X^{\text{sep}}$.*

Proof.

- (a) From [Kat01, Corollary of Theorem 3], we obtain an upper bound B on the sum of the ℓ -adic Betti numbers of X (which are unchanged by base extension to $\overline{\mathbb{F}}_q$). Then the

zeta function $Z_X(T)$ is a rational function of degree at most B . Compute $\#X(\mathbb{F}_{q^n})$ for $n \in \{1, 2, \dots, 2B\}$; this determines the mod T^{2B+1} Taylor expansion of $Z_X(T)$, which is enough to determine $Z_X(T)$. Then $\dim V_\mu$ is the number of complex poles λ of $Z_X(T)$ such that λ is a root of unity times q^{-p} , counted with multiplicity.

- (b) Algorithm B first runs algorithm A to compute $v_\mu := \dim V_\mu$, and then runs the algorithm of Corollary 8.4 until it prints v_μ , in which case algorithm B returns v_μ . If $T^p(X, \ell)$ and $E^p(X, \ell)$ hold, Proposition 7.5 implies that v_μ equals $\text{rk Num}^p X^{\text{sep}}$, and the algorithm of Corollary 8.4 eventually prints the latter, so algorithm B terminates with the correct output.

Assume $E^p(X, \ell)$. Proposition 7.5 implies that $\text{rk Num}^p X^{\text{sep}} \leq v_\mu$ with equality if and only if $T^p(X, \ell)$ holds. So if algorithm B terminates, then $T^p(X, \ell)$ holds. \square

Corollary 8.26. *There is an algorithm to compute $\text{NS } X^{\text{sep}}$ (in the same sense as Theorem 8.22(b)) and its subgroup $\text{NS } X$ for any nice variety X over a finite field such that $T^1(X, \ell)$ holds for some ℓ .*

Proof. Apply Theorem 8.25(b), using that $E^p(X, \ell)$ holds for $p = 1$, to obtain $\text{rk NS } X^{\text{sep}}$. Then Theorem 8.22(b) lets us compute the Galois module $\text{NS } X^{\text{sep}}$. By Proposition 6.2, computing its G -invariant subgroup yields $\text{NS } X$. \square

Corollary 8.27. *There is an unconditional algorithm to compute $\text{NS } X^{\text{sep}}$ and $\text{NS } X$ for any K3 surface X over a finite field of characteristic at least 5.*

Proof. By [Cha12, Corollary 2], $T^1(X, \ell)$ holds for these X . Apply Corollary 8.26. \square

ACKNOWLEDGEMENTS

We thank François Charles, Robin Hartshorne, Moshe Jarden, Andrew Kresch, Martin Olsson, and Burt Totaro for comments. We thank the Banff International Research Station, the American Institute of Mathematics, the Centre Interfacultaire Bernoulli, and the Mathematisches Forschungsinstitut Oberwolfach for their hospitality and support.

REFERENCES

- [And96] Yves André, *On the Shafarevich and Tate conjectures for hyper-Kähler varieties*, Math. Ann. **305** (1996), no. 2, 205–248, DOI 10.1007/BF01444219. MR1391213 (97a:14010) \uparrow 1
- [BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034) \uparrow 8.3
- [Cha11] François Charles, *On the Picard number of K3 surfaces over number fields*, November 17, 2011. Preprint, [arXiv:1111.4117v1](#). \uparrow 2
- [Cha12] ———, *The Tate conjecture for K3 surfaces over finite fields*, July 7, 2012. Preprint, [arXiv:1206.4002v2](#). \uparrow 1, 8.4
- [EGA IV₄] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. **32** (1967), 361 (French). MR0238860 (39 #220) \uparrow 8.3
- [Eis95] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. With a view toward algebraic geometry. MR1322960 (97a:13001) \uparrow 8.3
- [EJ11a] Andreas-Stephan Elsenhans and Jörg Jahnel, *On the computation of the Picard group for K3 surfaces*, Math. Proc. Cambridge Philos. Soc. **151** (2011), no. 2, 263–270, DOI 10.1017/S0305004111000326. MR2823134 (2012i:14015) \uparrow 2

- [EJ11b] ———, *The Picard group of a K3 surface and its reduction modulo p* , Algebra Number Theory **5** (2011), no. 8, 1027–1040. $\uparrow 2$
- [Got78] Gerd Gotzmann, *Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes*, Math. Z. **158** (1978), no. 1, 61–70 (German). MR0480478 (58 #641) $\uparrow 8.3$
- [Har88] Dan Haran, *Quantifier elimination in separably closed fields of finite imperfectness degree*, J. Symbolic Logic **53** (1988), no. 2, 463–469, DOI 10.2307/2274518. MR947853 (89i:03057) $\uparrow \text{civ}$
- [HKT12] Brendan Hassett, Andrew Kresch, and Yuri Tschinkel, *Effective computation of Picard groups and Brauer–Manin obstructions of degree two K3 surfaces over number fields*, March 10, 2012. Preprint, [arXiv:1203.2214v1](#). $\uparrow 2$
- [Her26] Grete Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), no. 1, 736–788, DOI 10.1007/BF01206635 (German). MR1512302 $\uparrow 8.3$, 8.3
- [IK99] Anthony Iarrobino and Vassil Kanev, *Power sums, Gorenstein algebras, and determinantal loci*, Lecture Notes in Mathematics, vol. 1721, Springer-Verlag, Berlin, 1999. Appendix C by Iarrobino and Steven L. Kleiman. MR1735271 (2001d:14056) $\uparrow 8.3$
- [Kah09] Bruno Kahn, *Démonstration géométrique du théorème de Lang–Néron et formules de Shioda–Tate*, Motives and algebraic cycles, Fields Inst. Commun., vol. 56, Amer. Math. Soc., Providence, RI, 2009, pp. 149–155 (French, with English and French summaries). MR2562456 (2010j:14083) $\uparrow 2$
- [Kat01] Nicholas M. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. **7** (2001), no. 1, 29–44. Dedicated to Professor Chao Ko on the occasion of his 90th birthday. MR1803934 (2002d:14028) $\uparrow a$
- [Kee08] Dennis S. Keeler, *Fujita’s conjecture and Frobenius amplitude*, Amer. J. Math. **130** (2008), no. 5, 1327–1336, DOI 10.1353/ajm.0.0015. MR2450210 (2009i:14006) $\uparrow 8.3$
- [Kle05] Steven L. Kleiman, *The Picard scheme*, Fundamental algebraic geometry, Math. Surveys Monogr., vol. 123, Amer. Math. Soc., Providence, RI, 2005, pp. 235–321. MR2223410 $\uparrow 6$
- [Klo07] Remke Kloosterman, *Elliptic K3 surfaces with geometric Mordell–Weil rank 15*, Canad. Math. Bull. **50** (2007), no. 2, 215–226, DOI 10.4153/CMB-2007-023-2. MR2317444 (2008f:14055) $\uparrow 2$
- [Lan56] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR0086367 (19,174a) $\uparrow 6$
- [Mau12] Daves Maulik, *Supersingular K3 surfaces for large primes*, April 7, 2012. Preprint, [arXiv:1203.2889v2](#). $\uparrow 1$
- [MP12] Daves Maulik and Bjorn Poonen, *Néron–Severi groups under specialization*, Duke Math. J. (2012). To appear. $\uparrow 2$
- [Mil80] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR559531 (81j:14002) $\uparrow 5$
- [Min87] H. Minkowski, *Zur Theorie der positiven quadratischen Formen*, J. reine angew. Math. **101** (1887), 196–202. $\uparrow 4.1$
- [Nér52] André Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d’une courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), 101–166 (French). MR0056951 (15,151a) $\uparrow 3$
- [Nyg83] N. O. Nygaard, *The Tate conjecture for ordinary K3 surfaces over finite fields*, Invent. Math. **74** (1983), no. 2, 213–237, DOI 10.1007/BF01394314. MR723215 (85h:14012) $\uparrow 1$
- [NO85] Niels Nygaard and Arthur Ogus, *Tate’s conjecture for K3 surfaces of finite height*, Ann. of Math. (2) **122** (1985), no. 3, 461–507, DOI 10.2307/1971327. MR819555 (87h:14014) $\uparrow 1$
- [Ogu09] Keiji Oguiso, *Shioda–Tate formula for an abelian fibered variety and applications*, J. Korean Math. Soc. **46** (2009), no. 2, 237–248, DOI 10.4134/JKMS.2009.46.2.237. MR2494474 (2009m:14011) $\uparrow 2$
- [SGA 6] *Théorie des intersections et théorème de Riemann–Roch*, Lecture Notes in Mathematics, Vol. 225, Springer-Verlag, Berlin, 1971 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1966–1967 (SGA 6); Dirigé par P. Berthelot, A. Grothendieck et L. Illusie. Avec la collaboration de D. Ferrand, J. P. Jouanolou, O. Jussila, S. Kleiman, M. Raynaud et J. P. Serre. MR0354655 (50 #7133) $\uparrow 3$

- [Shi72] Tetsuji Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), 20–59. MR0429918 (55 #2927) ↑2
- [Shi86] ———, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. **108** (1986), no. 2, 415–432, DOI 10.2307/2374678. MR833362 (87g:14033) ↑2
- [Shi90] ———, *On the Mordell-Weil lattices*, Comment. Math. Univ. St. Paul. **39** (1990), no. 2, 211–240. MR1081832 (91m:14056) ↑2
- [Tat76] John Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274. MR0429837 (55 #2847) ↑a
- [Tat94] ———, *Conjectures on algebraic cycles in l -adic cohomology*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 71–83. MR1265523 (95a:14010) ↑1, 7.2, 7.4, 7.2
- [Tat95] ———, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440. MR1610977 ↑2
- [vL07a] Ronald van Luijk, *$K3$ surfaces with Picard number one and infinitely many rational points*, Algebra Number Theory **1** (2007), no. 1, 1–15. MR2322921 (2008d:14058) ↑2
- [vL07b] ———, *An elliptic $K3$ surface associated to Heron triangles*, J. Number Theory **123** (2007), no. 1, 92–119, DOI 10.1016/j.jnt.2006.06.006. MR2295433 (2007k:14077) ↑2

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139-4307, USA

E-mail address: poonen@math.mit.edu

URL: <http://math.mit.edu/~poonen/>

MATHEMATICS INSTITUTE, UNIVERSITY OF WARWICK, COVENTRY, CV4 7AL, UNITED KINGDOM

E-mail address: adomani@gmail.com

URL: <http://homepages.warwick.ac.uk/~maskal/zone>

MATHEMATISCH INSTITUUT, UNIVERSITEIT LEIDEN, POSTBUS 9512, 2300 RA, LEIDEN, THE NETHERLANDS

E-mail address: rvl@math.leidenuniv.nl

URL: <http://www.math.leidenuniv.nl/~rvl/>